Attribute-based Storage Supporting Secure Deduplication Of Encrypted Data In Cloud

ABSTRACT

- Attribute-based encryption (ABE) has been widely used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider, and can share the data with users possessing specific credentials (or attributes).
- However, the standard ABE system does not support secure deduplication, which is crucial for eliminating duplicate copies of identical data in order to save storage space and network bandwidth.
- In this paper, we present an attribute-based storage system with secure deduplication in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage. Compared with the prior data deduplication systems, our system has two advantages. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys.
- Secondly, it achieves the standard notion of semantic security for data confidentiality while existing systems only achieve it by defining a weaker security notion.
- In addition, we put forth a methodology to modify a ciphertext over one access policy into ciphertexts of the same plaintext but under other access policies
- without revealing the underlying plaintexts

EXISTING SYSTEM

- A CP-ABE scheme that is proved to be secure under the standard model, but it only supports the AND access structures.
- Acp-abe system under more advanced access structures is proposed by based on the number theoretic assumption.
- In order to overcome the limitation that the size of the attribute space is polynomially bounded in the securi-ty parameter and the attributes are fixed ahead, rouselakis and waters built a large universe cp-abe system under the prime-order group.

DISADVANTAGE

- Key challenge in secure deduplication is to make it secure against duplicate faking attack
- A malicious user may intercept an outsourcing request and tamper with the ciphertext

PROPOSED SYSTEM

- we present an attribute-based storage system
- which employs ciphertext-policy attribute-based encryption (CP-ABE) and supports secure deduplication.
- Firstly, the system is the first that achieves the stan-dard notion of semantic security for data confiden-tiality in attribute-base deduplication systems by resorting to the hybrid cloud architecture

ADVANTAGES

- Achieve data consistency in the system.
- Storage system with secure deduplication
- It is impossible for an adversary to perform duplicate faking attacks

HARDWARE REQUIREMENTS

- System : PentiumIV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : windows XP/7
- Coding Language : ASP.net,C#/java

CONCLUSIONS

- Attribute-based encryption (ABE) has been widely used in cloud computing where data providers outsource their encrypted data to the cloud and can share the data with users possessing specified credentials.
- On the other hand, deduplication is an important technique to save the storage space and network bandwidth, which eliminates duplicate copies of identical data.
- However, the standardABE systems do not support secure deduplication, which makes them costly to be applied in some commercial storage services.
- In this paper, we presented a novel approach to realize an attribute-based storage system supporting secure dedupli-cation.